European Research Studies Journal
Volume XXVI, Issue 3, 2023

pp. 363-380

Blockchain-Based Certification: Enhancing Transparency and Trust in Higher Education

Submitted 15/07/23, 1st revision 10/08/23, 2nd revision 28/08/23, accepted 10/09/23

Krzysztof Saja[1], Adam Stecyk[2]

Abstract:

Purpose: *The aim of this paper is to showcase the practical application of the blockchain technology for the certification in the higher education.*
Design/Methodology/Approach: *The research methodology is based on the 5D model of educational entity, which consists of 5 main dimensions: the organizational, infrastructural, methodological social and economic. The main methods used in the paper include: subject studies, logical synthesis, system approach and process approach.,*
Findings: *A designed certification system utilizing blockchain technology can offer several technical advantages. Firstly, the decentralized and tamper-proof nature of blockchain ensures the security and integrity of the certification process. This eliminates the possibility of fraudulent activities and ensures the authenticity of the issued certificates. Additionally, the use of smart contracts can automate certification-related tasks, resulting in increased efficiency and accuracy while reducing the need for manual intervention. Secondly, the use of public blockchains in the certification system provides easy access and verification of certificate details for multiple parties.*
Practical Implications: *A blockchain-based certification system can provide a high level of security, integrity, and authenticity to the certification process. By utilizing the technology's decentralized and tamper-resistant nature, it can minimize the risk of fraud and increase the trustworthiness of the certification system. In addition to that, a well-designed certification system can provide numerous economic benefits. Firstly, it can streamline and optimize the certification process, reducing the costs associated with manual verification and other administrative tasks. This can save time and resources for both individuals and educational institutions, allowing them to focus on other important tasks.*
Originality/Value: *The originality of the study results from the synthesis of various research methods in the approach to certification processes in higher education.*

Keywords: *Blockchain, certification, higher education, quality, safety*.

JEL codes: *I25, I28.*

Paper type: *Research article.*

[1]*Assoc. Prof., University of Szczecin, Institute of Philosophy and Cognitive Science, krzysztof.saja@usz.edu.pl;*
[2]*Assoc. Prof., University of Szczecin, Institute of Spatial Management and Socio-Economic Geography, adam.stecyk@usz.edu.pl;*

1. Introduction

The quality and efficiency of education by offering educational services in Polish higher education is increasingly an effective tool for building a competitive advantage in the rapidly changing social and economic reality. The previous development of the information society (Lara 2022; Haleta *et al.,* 2022) and a knowledge-based economy (Durazzi, 2019) has led to the widespread use of general-purpose technologies such as computers, the Internet, and smartphones (Śledziewska and Włoch, 2020).

At the same time, it is assumed that these technologies form the basis of the innovation and development system. New solutions based on them may emerge over time, which can eventually become general-purpose technologies in many social and economic fields.

The consequence of these changes is another stage in the development of civilization, called the economy 4.0 (Costan *et al.,* 2021) and its founding technologies, which include cloud solutions (Spirin *et al.,* 2022), big data and business intelligence analytical technologies (Mittal *et al.,* 2022) blockchain technology (Raimundo and Rosario, 2021), the Internet of Things (Stead *et al.,* 2019) and broadly defined artificial intelligence (Li and Gu, 2023).

So the question arises about the impact of new technologies on modern higher education and the possibilities of their practical implementation to achieve specific educational goals (Stecyk, 2014). The literature in the field indicates that educational entities, understood as universities or specifically separated units such as departments or institutes, can undergo model decomposition, in order to configure key resources and coordinate main and auxiliary teaching processes (Toprak *et al.,* 2021).

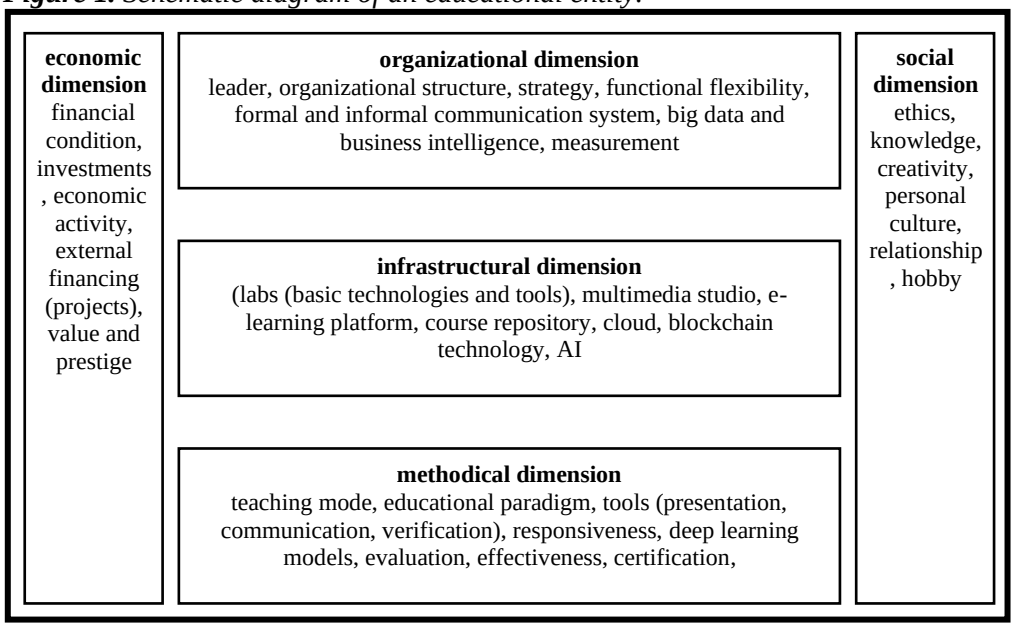
This approach allows for the identification and measurement of key factors determining the goal function, which is to raise (maintain) the level of quality and efficiency of teaching. At this point, it is necessary to consider how Polish universities can use innovative 4.0 technologies to increase their scientific and research potential and what implementation model of new solutions can be effective.

The schematic idea of the 5D educational entity is presented in Figure 1, which consists of 5 main dimensions: the organizational, infrastructure, and methodological dimensions are the main elements of the model, responsible for organizing work and securing the technical, technological, and methodological processes of teaching.

The social dimension, i.e., the education stakeholders such as students and organizational leaders, administrative and academic staff, plays a key role in the functioning of these dimensions. Efficient, effective and developmentally

functioning of the educational entity is ensured by the economic dimension, responsible for financial stability and investments. The division into specific dimensions is subjective and serves to distinguish individual factors determining the quality and effectiveness of education, which enables their measurement and evaluation (certification).
The proposed model is arbitrary; in real-life practice, the proposed dimensions overlap and it is difficult to unambiguously determine the boundaries between them. It is also assumed that the model is open and can be subjected to certain modifications in order to better fit a specific research object or to realize a specific task or educational process (Stecyk, 2018).

Figure 1. *Schematic diagram of an educational entity.*



Source: *Own elaboration.*

The 4.0 technologies are an important element of the 5D model and can be used in educational processes. A common solution in Polish higher education institutions is the use of cloud tools (Ciobanu and Zaharia, 2023) which offer certain, increasingly advanced information and communication services and applications, whose efficiency increases with the development of traditional online services and the increase in data transfer speed.

Business intelligence software is also gaining popularity (Fowler, 2019) which, combined with the concept of big data (Youshan *et al.*, 2021) allows for a new approach to analyzing business data and, particularly important for the quality of educational data.

Another emerging technology in education is blockchain, which can provide a secure and decentralized system for storing and sharing educational data, such as student transcripts and certificates, without needing a central authority Dudder *et al.,* 2021). This can improve the transparency, security, and efficiency of educational processes. One potential use case for blockchain in education is the creation of digital credentials (Deenmahomed *et al.,* 2021). Traditionally, universities and other educational institutions store and issue student credentials such as degrees and certificates.

However, with blockchain technology, students can have their credentials stored on a decentralized ledger, making it easy for them to share their achievements with potential employers and other institutions (Maestre *et al.,* 2022)

2. A Comprehensive Overview of Blockchain Technology

Blockchain technology is best understood in the context of the evolution of the Internet. Web 1.0 refers to the first stage of the World Wide Web evolution. This decentralized, static web offered limited functionality, basic design, and simple user experience. It consisted of simple HTML files that provided information, but users could not interact with them or provide their content. Web 2.0 emerged in the early 2000s and marked a significant web development shift.

It introduced a more interactive and engaging user experience, emphasizing user-generated content, social networking, and collaboration. Web 2.0 is commonly referred to as the "Social Web." Popular tech companies and applications such as Facebook, YouTube, Instagram, Twitter, Netflix, and Spotify represent its mature form.

The narrative that blockchain is a base for the new Internet revolution was gathering popularity from the beginning of the blockchain technology (Tapscott and Tapscott, 2016). The phrase Web 3.0 started to gain attention in 2017 and became popular in blockchain communities in 2021 (Voshmgir, 2020; Tante, 2021; Smorenburg, 2021). In those narratives, Web 3.0 is seen as a blockchain-based backend infrastructure layer on top of existing network technologies that aims to restructure the Internet in a decentralized way.

While the user interfaces of Web 3.0 look familiar and are built with the same frontend, client-side technology, they no longer get their crucial content from centralized servers but from blockchain-based content providers. This increases security, transparency, and immutability, benefiting users and businesses.

Another critical technological feature of Web 3.0 is that it’s stateful by design. In Web 2.0, centralized databases became the mainstream form of data storage and management: the state is only placed in some network nodes controlled by

individual parties. The Web3 state is partially based on a blockchain protocol. Multiple network nodes share it, persist its history, and it's accessible by anyone.

Web 3.0 is also based on the capability of writing scripts or backend programs called smart contracts that are accessed and executed on Distributed Ledger Technology (DLT) such as Ethereum and many more. Contract owners can modify them according to publicly transparent rules and can have their own internal state that is usually represented by cryptographically secured tokens.

Tokens can represent some value that can be owned and usually transferred. Blockchain state, in the form of a token or smart contract, can be seen as a value (like Bitcoin that started to be exchanged in 2010) or represent some other valuable things, like a higher education certificate. Ownership of such tokens can be transferred and exchanged. Blockchain state is therefore usually decentralized, ownable, and tradable.

The public Blockchain state is also easily accessed and compositable. Every smart contract can publish at least part of its internal state and methods, which can be read and executed by other contracts created by third parties. Tokens issued by smart contracts represent their internal state fully controlled by their owners (wallets).

Other contracts can use those tokens to create a meta state, which can be called meta tokens. Such derivatives tokens and contracts can reuse existing smart contracts scripts published by others. This is the basis of a quickly developed Web 3.0 ecosystem that creates whole new public markets and a token economy.

From a technical perspective, every token that can be transferred from wallet to wallet can also be sold and bought. There are already decentralized exchanges that specialize in this process. This is one more important innovation. Web3 application can allow you to monetize your content using external, third-party services.

For example, you can create a digital art image, music sample, in-game gadget, blog post, or research article as an Ethereum ERC-721 NFT token, publish it on a chain, sell it on “OpenSea” NFT auction platform, buy it later on “Rarible”, and then benefit from every future transaction or even views of your content, also outside the initial application.

You can create an ERC-20 token as a utility token for your new Web3 application, which can be bought on a decentralized exchange, transferred, staked, borrowed, or used as loan collateral in any other relevant decentralized application owned or will be held by someone else.

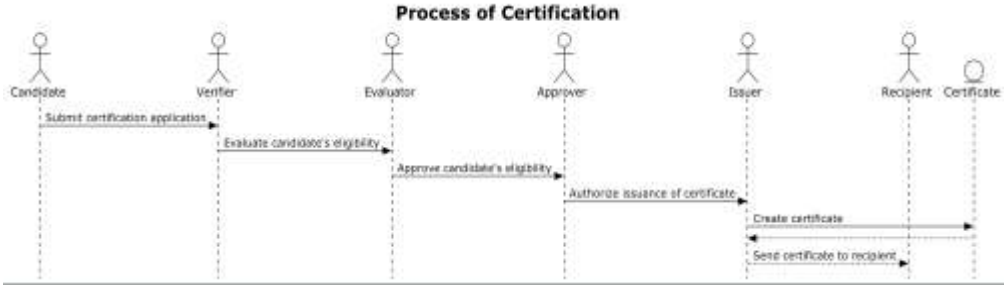
DLT is one of many technologies needed for Web 3.0. A multitude of other protocols is required to create a decentralized application. However, “blockchain” seems to be a synonym for many Web 3.0 protocols or Web 3.0 itself.

Apart from computation, we need file storage, messaging, identities, external data (so-called "oracles"), and many other decentralized services. A blockchain network is a shared „processor" and "memory" for decentralized applications that operate on top of it. It is a distributed accounting machine recording all token transactions and performing computations.

3. Secure, Transparent, and Verifiable: The Blockchain Model of Certification

A typical certification process contains several steps and key actors involved, as shown in the diagram below.

Figure 2. *Simplified process of certification*



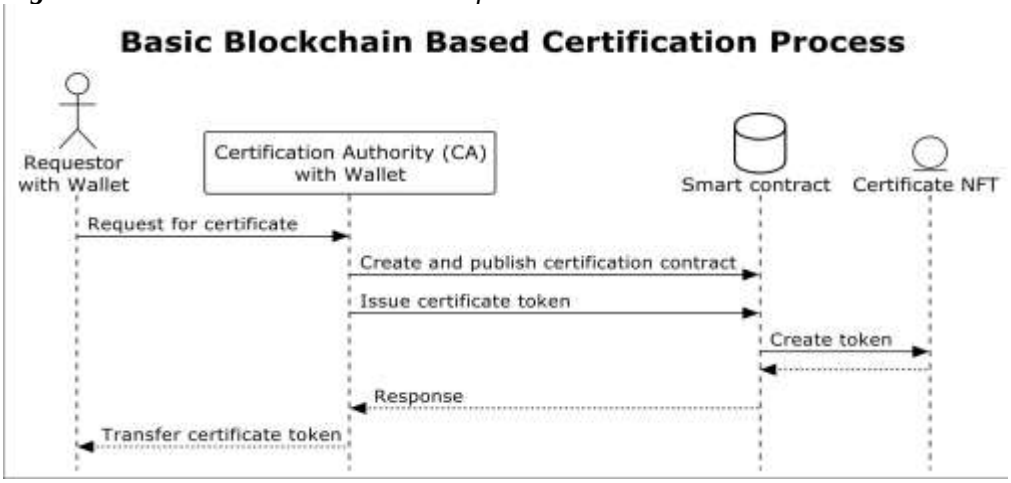
Source: *Own elaboration.*

The key actors in this process are the Candidate, Verifier, Evaluator, Approver, Issuer, and Recipient. The Candidate is the individual seeking certification, and their role is to apply for certification. The Verifier is responsible for verifying the candidate's eligibility and forwarding the application to the Evaluator if the candidate meets the requirements.

The Evaluator evaluates the candidate's eligibility and approves the application if it meets the necessary criteria. The Approver authorizes the certificate issuance, creates it, and sends it to the Recipient. In real live scenarios, multiple described roles can be shared and conveyed by a different group of actors or even represented by only two persons: Certificate Issuer and Certificate Recipient.

In the context of blockchain-based certification, the process of issuing a certificate typically involves several steps that are represented in the following diagram. The process of certification using blockchain involves three main players: the Requestor with Requestor Wallet, the Certification Authority (CA) with Wallet, and the Blockchain platform with smart contract capabilities. Two involved parties need to have their blockchain wallets. CA needs to have CA Wallet to initialize the tokenization process by creating a certification smart contract and further manage its state. To transfer the issued certificate to Recipient, CA also needs to know at last public address of the Recipient's wallet.

Figure 3. *Basic Blockchain-Based Certification Process*



Source: *Own elaboration.*

The Requestor initiates the process by requesting a certificate from the Certification Authority. The Certification Authority, using its CA Wallet, creates and publishes a certification contract on the chosen blockchain. By signing transactions via CA Wallet, CA will fully control the certification contract and have administrative rights over the issued certificates.

Once the contract is published, the Certification Authority can issue a certificate token through the contract and transfer the certificate to the public address of the Requestor wallet. The issued certificate should contain information about the certificate and the Recipient. The information about the Recipient, e.g., his name, place, and date of birth, is needed to be able to validate if the certificate's future owner was the initial Recipient of the certificate. That information can be publicly written in the certificate metadata or used only as input for creating and storing a unique Recipient identity hash string that can be recreated and validated only by those who know that personal information beforehand.

It's important to note that the certificate token is not stored directly in the Requestor or CA wallet but always on the public blockchain. The CA Wallet is critical to the certification process because it should have some administrative rights over the contract and issued tokens. It's owned and controlled by the Certification Authority, which must ensure its security.

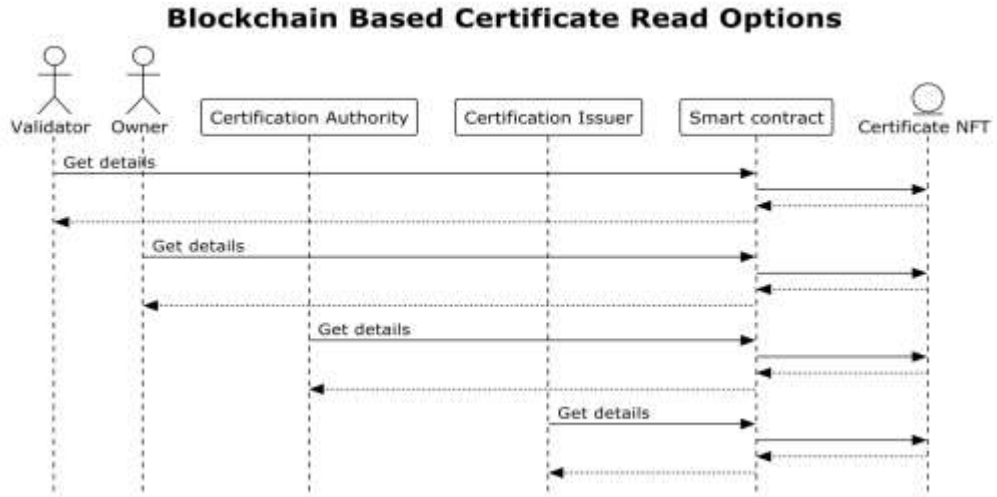
To do so, they should choose a reputable wallet provider, store it securely, and limit access to authorized personnel. Another essential aspect of securing the wallet is using a seed phrase, a unique combination of words that recreates the wallet. In case of loss or damage, the seed phrase can restore the wallet and recover ownership of certification contracts, so it must be kept secure.

In addition to using a seed phrase, regular backups and audits should be conducted to ensure the certificates' integrity and availability. Using a blockchain-based wallet adds another layer of security, as the decentralized nature of the blockchain makes it nearly impossible to modify or tamper with certificates without detection.

When a certificate is created and recorded on a public blockchain, it becomes easily accessible and verifiable by multiple parties. In addition to the Requestor and the Certification Authority, other parties such as potential employers or educational institutions may want to validate the certificate's authenticity.

This is possible because the certificate is stored as a tamper-proof record on the public block chain. It can be visualized in the following diagram:

Figure 4. *Blockchain-Based Certificate Read Options*



Source: *Own elaboration.*

The Requestor, Certification Authority, and Issuer can access the certificate details through the smart contract. They can review the certificate to ensure its accuracy and to confirm that it has not been tampered with.

Using a public blockchain makes the certificate a permanent and accessible record that multiple parties can easily read. This provides added trust and confidence in the certification process (Hawlitschek, 2018; Bratspies, 2018; Teng, nd; Rehman *et al.,* 2020) as anyone can validate the certificate's authenticity without relying solely on the issuer or the Requestor.

The validation process involves accessing the certificate information from the blockchain using smart contract features. Validators, including potential employers or educational institutions, can query the blockchain for certificate details by

invoking the designed smart contract certification methods. This allows them to read the certificate and verify its authenticity.

The process of validating a public certificate on the blockchain requires the validator to confirm that the certificate is authentic and has not been tampered with. The risk of fraudulent certificates can be mitigated using a Trusted Certification Repository, a list of verified contract addresses that issue valid certificates. Validators can verify the authenticity of a certificate contract address by checking it against this repository, either stored as plain text or through a Smart Contract, which can be easily designed and implemented to handle such Trusted Certification Repository functionality.

To validate a certificate, the certificate owner must provide the Validator with the certificate address and their own identity. The validator checks the certificate contract address against the Trusted Certification Repository to confirm its authenticity and retrieves the certificate details from the blockchain. This ensures that the certificate was issued by the genuine Certification Authority.

However, validating the certification information is not enough to verify that the current certification owner was the initial Recipient of the certificate. Validators must have a way to link the certificate to the actor claiming to be the Recipient. In order to answer this question, we need to compare the Recipient identity information stored in the certificate with one provided to the Validator.

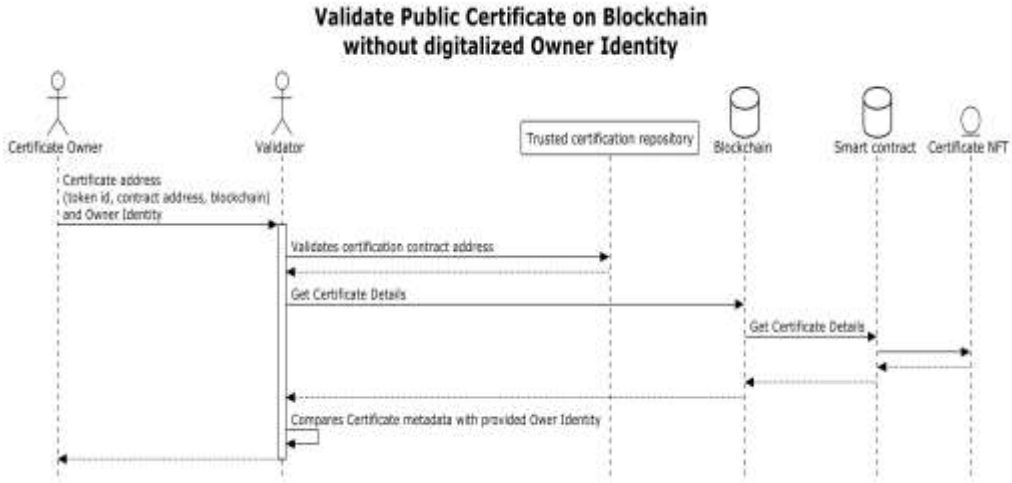
Validator must compare the certificate metadata, containing publicly visible or hashed personal information of the Recipient, with the provided owner identity or its hashed version. If the certificate information about Recipient matches the Certificate Owner, the ownership is verified, and the Validator can confirm that the certificate belongs to the current owner. Described process can be visualized in the following diagram:

The basic model of blockchain certification presented above provides a framework for understanding the process. However, this model needs more complexity to handle the diverse and nuanced certification requirements. In this chapter, we present a more sophisticated model of certification to illustrate the key steps involved. It describes the usage of a dedicated Certification Platform Service necessary for handling all the non-trivial and technical steps involved. The Certification Platform is a specialized software solution designed to handle the complex requirements of certification processes.

This custom-built software was not described in other papers yet. An overview of other blockchain-based certification systems is done in (Maestre *et al.*, 2022). The presented Certification Platform is built mainly in TypeScript programming language, Angular frontend Framework, Nest.js backend Framework, and Postgres SQL Database. It's run in a Node.JS JavaScript environment. Smart contracts were

developed with the help of the Hardhat framework and in Solidity Smart Contract Scripting Language. Certification contracts and tokens can be published on multiple EVM-compatible blockchains.

Figure 5. *Validate Public Certificate without Digitalized Owner Identity*



Source: *Own elaboration.*

In higher education, issuing multiple certificates to a group of individuals, such as degrees, diplomas, and other credentials is common. Organizing and presenting these certificates in a visually appealing and easy-to-access manner is important. Typically, certificates are part of a certification program created for multiple recipients and are rarely created outside of such a program.

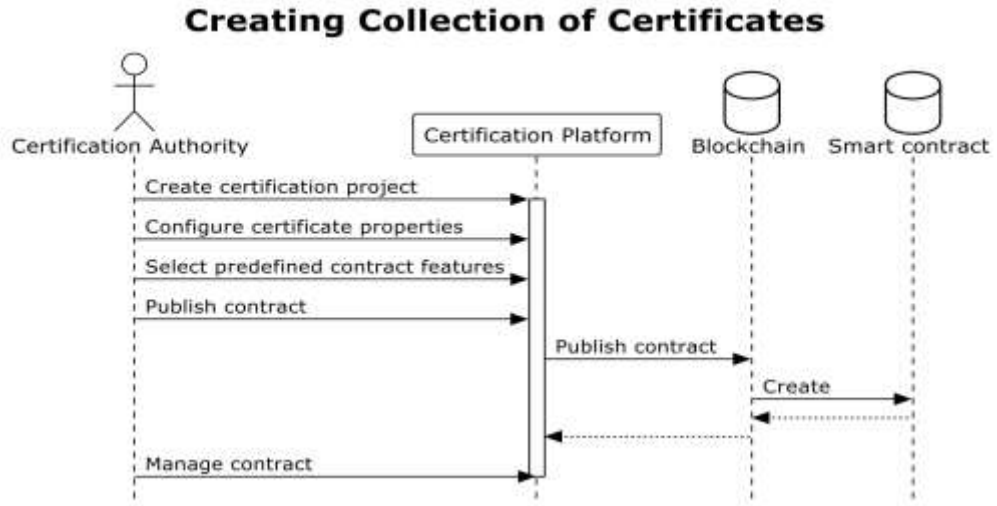
Therefore, the following diagram outlines the process of creating a collection of certificates, including references to certification artwork, metadata, and the blockchain. This process ensures that certificates are efficiently produced, easily managed, and securely stored.

The diagram above illustrates the key steps in creating a collection of certificates using blockchain technology. The process begins with the Requestor, who initiates a request for certification. The Certification Authority receives the request and creates a certification project on the Certification Platform.

The Certification Authority configures the certificate properties, such as the certification artwork and metadata, and selects predefined contract features before publishing the contract. The artwork and metadata can be customized or even generated with the help of the User Interface. The project owner can create a selected number of unique images or backgrounds that visually represent the certificates using generative art, which creates unique artwork based on configurable

algorithms and provided properly layered pictures. This art-backed or enhanced certificate provides important motivational and gamification advantages.

Figure 6. *Creating Collection of Certificates*



Source: *Own elaboration.*

In addition, the Certification System allows the configuration of certification metadata that will be referenced in the certification token. The artwork and metadata are then securely stored in a decentralized, tamper-proof storage platform like IPFS. Once the artwork and metadata have been configured and the smart contract templates have been selected, with their parameters set for the specific certification collection, the Issuer publishes the contract on the blockchain.

After publishing the contract, it is ready to mint a certification token for the Recipient. The Authority can invoke the contract functions, such as "*mint*" ensuring that all requirements and criteria are met, by using a simple graphical interface in the Certification Platform, calling the Certification Platform REST API endpoint directly by its internal system, or invoking the method using whatever publicly available method to interact with the Smart Contract on selected blockchain by signing the transaction message by the Wallet.

The Certificate NFT is the final product of the certification process, representing the candidate's achievement of the requirements and criteria. The Certificate NFT references the Issuer and Recipient identity and other metadata, such as certification artwork, which can visually represent the certificate.

Several features should be considered to create a robust and secure system for blockchain certificates. Below we will discuss only the most important features we believe the blockchain certification system should take into consideration:

1. **Public Access:** Certificates are crucial in verifying an individual's skills or achievements. It is important that certificates are easily accessible to interested parties and can be easily validated. The certificate recipient should be able to prove the authenticity of their certification to anyone who wants to validate the certificate. Additionally, the certification gallery should be shareable on popular applications and platforms in the Web3 space. Therefore, selecting public, well-recognized blockchains for certification is recommended rather than private, close-gated DLTs as in other blockchain certification propositions (Zhao and Si, 2022).

2. **Modularized and Open Approach**: Smart contracts and certificates can be utilized in future Web3 applications and should be treated as the first element of a modularized system of automatic management of achievements via certification, built and owned by any third-party software company. The certification model should be close to the most important industry standards to fulfill this requirement. Currently, the leader of such standards is the Ethereum blockchain and other blockchains that implement the Ethereum Virtual Machine (EVM) and well-recognized contract interfaces described in multiple relevant Ethereum Improvement Proposals (Various, 'Ethereum Improvement Proposals'). In order to easily evaluate implemented standards, the certification contract should implement a Standard Interface Detection mechanism (Christian Reitwießner *et al.,* 2018).

3. **Certificate as a Non-Fungible Token**: Blockchain certificates can be implemented in various ways, with any data structure and managing functions in a smart contract. However, to integrate with the overall philosophy and ecosystem of Web3, certificates should be implemented as tokens. Token standards are described in ERC-20 (Fabian Vogelsteller and Vitalik Buterin, 2015) ERC-777 (Jacques Dafflon *et al.,* 2017) ERC-721 (William Entriken *et al.,* 2018) and ERC-1155 (Witek Radomski *et al.,* 2018). Since the Certification Authority always issues certificates for a unique recipient in a specific context and time, the certificate must be treated as a non-fungible token (NFT). The certificate is recommended to be best represented by the ERC-721 or ERC-1155 standard with a „*tokenID"* and „*tokenURI"* properties that reflect its characteristics.

4. **Ownership**: The Certification Authority should have administrative rights over the certification contract. These administrative powers should be easily recognized and transferred to different wallets of CA if needed. Therefore, the contract is proposed to implement Contract Ownership Standard ERC-173 (Nick Mudge and Dan Finlay, 2018).

5. **Issuing and Revoking Mechanism**: In a typical certification process, the Certification Authority should be able to issue a certificate, also known as "minting" in a token context and revoke the certificate. Certificates can be

revoked for several reasons, such as misrepresentation, non-compliance, expiration, misconduct, criminal conviction, change in circumstances, or failure to pay fees. Therefore, the Certification Authority should be able to destroy the certificate. The simplest and most transparent solution for every party seems to be implementing ERC-5679: Token Minting and Burning standard (Tim Daubenschütz and Anders, 2022)

6. **CA and Recipient Identification**: The certificate token should have all the important information to identify the Certification Authority and the certificate recipient. The best solution would be to append such information in a standard that automatically verifies that the current token owner is the certification recipient.

7. **Certification Transfer Mechanism**. One of the approaches to whether certificates should be transferred and even sold on the secondary market is to recognize that a certificate is always issued to a Recipient and should not be used by any third party by design, even if that third party is a token owner. Only the certificate Recipient should be a party that can use the certificate to acknowledge merits that were certified by the CA. One approach that we considered was to use soul-bound tokens or non-transferable tokens described in Minimal Soulbound NFT (ERC-5192 (Tim Daubenschütz and Anders, 2022) or Consensual Soulbound Tokens (ERC-5484 (Buzz Cai, 2022).

However, if a validator can check if an actor is the genuine certificate recipient, there is no reason to disallow the transfer of tokens from wallet to wallet. Token holders usually have multiple wallets, and it is a good practice to manage them by filtering and transferring tokens from one wallet to another.

Moreover, blockchain wallets are still heavily developed, and it would be against good security practice to prevent token movement from an old and insecure wallet to a new and more robust wallet in the future. Also, the ability to trade certificates can be a reasonable idea. Some certificates, e.g. of well-known people and celebrities, from the context of important historical moments or certificates with attached artwork designed by a famous artist, can have market value as collectibles, even if the owners are not recognized as certification recipients. Therefore, we recommend not preventing token transfers from wallet to wallet.

4. Discussion: Certification Systems and Blockchain – Examining the Benefits and Limitations

A designed certification system utilizing blockchain technology can offer several technical advantages. Firstly, the decentralized and tamper-proof nature of blockchain ensures the security and integrity of the certification process. This eliminates the possibility of fraudulent activities and ensures the authenticity of the issued certificates.

Additionally, the use of smart contracts can automate certification-related tasks, resulting in increased efficiency and accuracy while reducing the need for manual intervention. Secondly, the use of public blockchains in the certification system provides easy access and verification of certificate details for multiple parties.

The information stored on the blockchain is transparent and easily accessible, eliminating the need for intermediaries and reducing the time and cost associated with verification. This can be particularly advantageous for employers, as they can quickly verify the authenticity of a candidate's certificate, saving them time and effort in the hiring process.

Furthermore, the decentralized nature of blockchain technology and its use of cryptographic protocols make it highly resistant to tampering and fraud. The storage of certificates on a public blockchain also makes them less vulnerable to being lost or destroyed. Additionally, using trusted certification repositories can help minimize the risk of fraudulent certificates. Automating this process with smart contracts can create a network of interconnected and hierarchical repositories for trusted certification programs.

Overall, a blockchain-based certification system can provide a high level of security, integrity, and authenticity to the certification process. By utilizing the technology's decentralized and tamper-resistant nature, it can minimize the risk of fraud and increase the trustworthiness of the certification system.

In addition to that, a well-designed certification system can provide numerous economic benefits. Firstly, it can streamline and optimize the certification process, reducing the costs associated with manual verification and other administrative tasks. This can save time and resources for both individuals and educational institutions, allowing them to focus on other important tasks.

Additionally, a trusted and efficient certification system can increase the value of credentials, leading to greater opportunities for individuals to advance their careers and increase their earning potential. Moreover, a well-designed certification system can help reduce fraud and increase trust in qualifications, increasing the overall economic value of the certification industry.

Furthermore, using NFT certificates can enhance the motivation of participants to learn and acquire new certificates. By linking certificates with artworks that can be displayed in a personal gallery, individuals can take pride in their achievements and display their skills uniquely and creatively.

Additionally, NFT certificates can be used in various applications developed by third parties, such as games, virtual social clubs, token-gated communities, and tickets, which can further expand the potential uses and value of the certificates. Employers and other organizations can make better-informed decisions by providing

a more accurate and reliable way to verify credentials, leading to better hiring practices and overall economic growth.

Although there are many benefits, implementing blockchain technology also has limitations and may encounter certain difficulties. These include blockchain wallet security, smart contract vulnerabilities, scalability, interoperability, and complexity.

To address these problems, it is crucial to choose a blockchain that can handle the expected volume of transactions, ensure adequate security measures are in place to prevent loss or theft of certificates, thoroughly test and audit smart contracts to identify and mitigate potential vulnerabilities and provide adequate education and training to users on how to use the blockchain-based certification system.

The adoption of blockchain technology may also lead to social issues. Firstly, there is a risk of exclusion of people unfamiliar with blockchain technology who may find it challenging to access or use the certification system. This may disproportionately affect certain groups of people, such as those with less technological proficiency, leading to a digital divide.

Secondly, there is a risk of bias against certain groups of people, such as those who do not have access to blockchain technology. This can lead to the perpetuation of existing inequalities and discrimination. Additionally, the public nature of the blockchain may make some candidates uncomfortable with the idea of their personal information being publicly available, leading to potential privacy concerns.

The incorporation of blockchain technology in the certification system is not without its economic challenges. Firstly, adopting blockchain technology can be expensive, especially for smaller organizations or candidates, which may be financially constrained. This could pose a significant barrier to their ability to implement the system and leverage its advantages.

Secondly, the cost of using the certification system may lead to unequal access, where certain groups of people may be unable to afford or use the system, potentially leading to their exclusion. Furthermore, there is a risk of dependency on the blockchain certification system, which can lead to potential problems if the system becomes unavailable or discontinued. This can result in candidates and organizations losing their valuable certification data and disrupting their processes.

In conclusion, creating a secure, scalable, interoperable, and user-friendly blockchain-based certification system requires addressing various technical, security, social, and economic challenges. Addressing these challenges can help create a certification system that benefits students and educational institutions by offering a reliable, tamper-proof, and easy-to-use platform for managing and verifying certifications. This can lead to a more efficient and trustworthy educational credentialing system that provides value to stakeholders and society at large.

References:

Bratspies, M.R. 2018. Cryptocurrency and the Myth of the Trustless Transaction. Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3141605. doi: 10.2139/ssrn.3141605.

Buzz Cai. 2022. ERC-5484: Consensual Soulbound Tokens. Ethereum Improvement Proposals, Aug. 17. https://eips.ethereum.org/EIPS/eip-5484.

Christian Reitwießner, Nick Johnson, Fabian Vogelsteller, Jordi Baylina, Konrad Feldmeier, William Entriken. 2018. ERC-165: Standard Interface Detection. Ethereum Improvement Proposals, Jan. 23. https://eips.ethereum.org/EIPS/eip-165.

Ciobanu, C.R., Zaharia, A. 2020. Impact of Cloud Mobile Solutions in the Education System. In: Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development During Global Challenges, K.S. Soliman, Ed., Norristown: Int Business Information Management Assoc-Ibima, 6145-6154.

Costan, E., et al. 2021. Education 4.0 in Developing Economies: A Systematic Literature Review of Implementation Barriers and Future Research Agenda. Sustainability, vol. 13, no. 22, p. 12763. doi: 10.3390/su132212763.

Deenmahomed, M.A.H., Didier, M.M., Sungkur, K.R. 2021. The future of university education: Examination, transcript, and certificate system using blockchain. Comput. Appl. Eng. Educ., vol. 29, no. 5, 1234-1256. doi: 10.1002/cae.22381.

Dudder, B., et al. 2021. Interdisciplinary Blockchain Education: Utilizing Blockchain Technology From Various Perspectives. Front. Blockchain, vol. 3, p. 578022. doi: 10.3389/fbloc.2020.578022.

Durazzi, N. 2019. The political economy of high skills: higher education in knowledge-based labour markets. J. Eur. Public Policy, vol. 26, no. 12, 1799-1817. doi: 10.1080/13501763.2018.1551415.

Electronic Commerce Research and Applications, vol. 29, 50-63. doi: 10.1016/j.elerap.2018.03.005.

Fabian Vogelsteller, Vitalik Buterin. 2019. ERC-20: Token Standard. Ethereum Improvement Proposals, Nov. 19. https://eips.ethereum.org/EIPS/eip-20.

Fowler, J. 2019. Business Intelligence at the University. In 2019 6th International Conference on Computational Science and Computational Intelligence (CSCI 2019), New York, 821-825. doi: 10.1109/CSCI49370.2019.00156.

Haleta, Y., Fursykova, T., Kozlenko, V., Habelko, O., Radchenko, M. 2022. Man of the information society: problems of formation and development. Cuest. Politicas, vol. 40, no. 75, 483-497. doi: 10.46398/cuestpol.4075.29.

Hawlitschek, F., Notheisen, B., Teubner, T. 2018. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy.

Jacques Dafflon, Jordi Baylina, Thomas Shababi. 2017. ERC-777: Token Standard. Ethereum Improvement Proposals, Nov. 20. https://eips.ethereum.org/EIPS/eip-777.

Lara, T.G. 2022. Learning in the Information Society: Alternatives for Theoretical Exploration. REV. CONRADO, vol. 18, no. 89, 208-215.

Li, S., Gu, X. 2023. A Risk Framework for Human-centered Artificial Intelligence in Education: Based on Literature Review and Delphi-AHP Method. Educ. Technol. Soc., vol. 26, no. 1, 187-202. doi: 10.30191/ETS.202301_26(1).0014.

Maestre, J.R., Bermejo Higuera, J., Gámez Gómez, N., Bermejo Higuera, R.J., Sicilia Montalvo, A.J., Orcos Palma, L. 2022. The application of blockchain algorithms to the management of education certificates. Evol Intell, 1-18. doi: 10.1007/s12065-022-00812-0.

Mittal, P., Kaur, A., Jain, R. 2022. Online Learning for Enhancing Employability Skills in Higher Education Students: The Mediating Role of Learning Analytics. TEM J., vol. 11, no. 4, 1469-1476. doi: 10.18421/TEM114-06.

Nick Mudge, Dan Finlay. 2018. ERC-173: Contract Ownership Standard. Ethereum Improvement Proposals, Jun. 07. https://eips.ethereum.org/EIPS/eip-173.

Raimundo, R., Rosario, A. 2021. Blockchain System in the Higher Education. Eur. J. Invest. Health Psychol. Educ., vol. 11, no. 1, 276-293. doi: 10.3390/ejihpe11010021.

Rehman, H.M., Salah, K., Damiani, E., Svetinovic, D. 2020. Trust in Blockchain Cryptocurrency Ecosystem. IEEE Transactions on Engineering Management, vol. 67, no. 4, 1196-1212. doi: 10.1109/TEM.2019.2948861.

Śledziewska, K., Włoch, R. 2020. Gospodarka cyfrowa. Jak nowe technologie zmieniają świat. Warsaw University Press. doi: 10.31338/uw.9788323541943.

Smorenburg, M. 2021. In Code We Trust: Bitcoin, Blockchain, Cryptocurrencies, Web3.0-A Revolution Governed by Rules, Not by Rulers, 1st edition. House of Qunard.

Spirin, M.O., Oleksyuk, P.V., Kasyan, P.S., Antoshchuk, S. 2022. Deployment and Administration of the Cloud Platform Google Workspace for Education in an Institution of Higher Education. Inf. Technol. Learn. Tools, vol. 92, no. 6, 172=197. doi: 10.33407/itlt.v92i6.5078.

Stead, M., Coulton, P., Lindley, J. 2019. Spimes Not Things: Creating a Design Manifesto for a Sustainable Internet of Things. Des. J., vol. 22, 2133-2152. doi: 10.1080/14606925.2019.1594936.

Stecyk, A. 2014. Wartość systemów e learningowych w podmiotach edukacyjnych. Szczecin: Difin.

Stecyk, A. 2018. Społeczno-gospodarcze efekty doskonalenia jakości usług edukacyjnych w szkolnictwie wyższym. Ekonomiczne Problemy Usług, vol. 130, 183-192. doi: 10.18276/epu.2018.130-18.

Tante. 2021. The Third Web. Nodes in a social network, Dec. 17. https://tante.cc/2021/12/17/the-third-web/.

Tapscott, D., Tapscott, A. 2016. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Portfolio, 2016.

Tim Daubenschütz and Anders. 2022. ERC-5192: Minimal Soulbound NFTs. Ethereum Improvement Proposals, Jul. 01. https://eips.ethereum.org/EIPS/eip-5192.

Toprak, M., Bayraktar, Y., Erdogan, A., Kolat, D., Sengul, M. 2021. New Generation University: A Model Proposal. Yuksekogretim Derg., vol. 11, no. 2, 344-362. doi: 10.2399/yod.21.210226.

Teng, Y. nd. What does it mean to trust blockchain technology? Metaphilosophy, vol. n/a, no. n/a, doi: 10.1111/meta.12596.

Various, 'Ethereum Improvement Proposals', Ethereum Improvement Proposals. https://eips.ethereum.org/.

Voshmgir, S. 2020. Token Economy: How the Web3 reinvents the Internet, Second edition. Berlin: Shermin Voshmgir, BlockchainHub Berlin.

William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs. 2018. ERC-721: Non-Fungible Token Standard. Ethereum Improvement Proposals, Jan. 24. https://eips.ethereum.org/EIPS/eip-721.

Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therien, Eric Binet, Ronan Sandford. 2018. ERC-1155: Multi Token Standard. Ethereum Improvement Proposals, Jun. 17. https://eips.ethereum.org/EIPS/eip-1155.

Youshan, Z., Shaozhe, G., Yong, L., Kaikai, Y., Qiming, L. 2021. Research Hotspots and Trend Analysis of Big Data in Education. In 2021 International Conference on Big Data Engineering and Education (BDEE 2021), New York, 110-114. doi: 10.1109/BDEE52938.2021.00026.

Zhao, X., Si, W.Y. 2023. NFTCert: NFT-Based Certificates With Online Payment Gateway. arXiv, Feb. 18, 2022. Available: http://arxiv.org/abs/2202.09511.